

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-198636

(43)公開日 平成10年(1998)7月31日

(51)Int.Cl. <sup>a</sup>	識別記号	F I	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
17/60		H 0 4 M 11/08	
H 0 4 L 9/32		3/42	Z
H 0 4 M 11/08		G 0 6 F 15/21	3 4 0 B
// H 0 4 Q 7/38		H 0 4 L 9/00	6 7 1
		審査請求 未請求 請求項の数10 O L (全 19 頁)	最終頁に続く

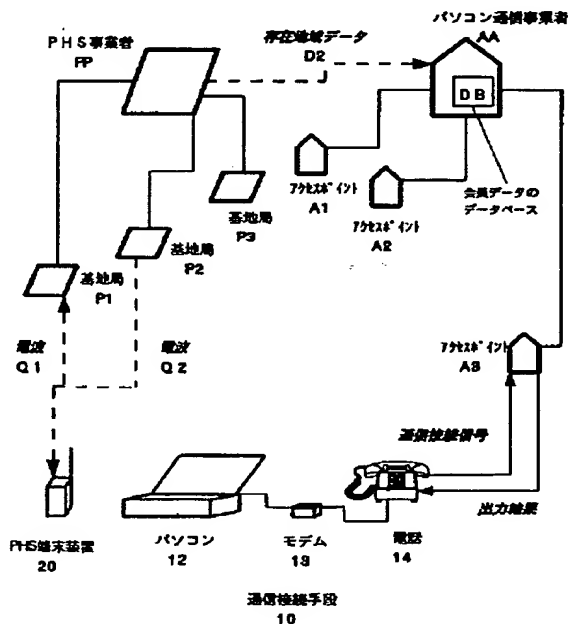
(21)出願番号	特願平9-3420	(71)出願人	000155469 株式会社野村総合研究所
(22)出願日	平成9年(1997)1月13日		東京都中央区日本橋1丁目10番1号
		(72)発明者	藤元 健太郎 横浜市保土ヶ谷区神戸町134番地 株式会 社野村総合研究所内
		(74)代理人	弁理士 黒田 博道 (外4名)

(54)【発明の名称】 個人認証システムおよび個人認証方法

(57) 【要約】

【目的】 正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない認証技術を提供する。

【構成】 会員ユーザに関する会員データ（例えば、会員の住所または居所）を読み込む会員データ読込手段、会員ユーザが所有するPHS端末装置(20)の存在地域データ(D2)をPHS事業者(PP)から取得する存在地域データ取得手段、会員データと存在地域データ(D2)との一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力手段を備える。



## 【特許請求の範囲】

【請求項1】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザに関する会員データを記憶する会員データ記憶手段、会員データを読み込む会員データ読込手段、会員ユーザが所有するPHS端末装置の存在地域データをPHS事業者から取得する存在地域データ取得手段、会員データと存在地域データとの一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者からの利益享受を継続できるとともに、不一致の場合にはサービス提供者からの利益を取得できないような出力結果を出力する出力手段を備えたことを特徴とする個人認証システム。

【請求項2】サービス提供者をパソコン通信事業者とし、会員データは、パソコン通信の接続電話番号によって認識することとしたことを特徴とする請求項1記載の個人認証システム。

【請求項3】会員データは、パソコン通信会員がパソコン通信の接続時に入力することとしたことを特徴とする請求項2記載の個人認証システム。

【請求項4】演算の結果が不一致の場合にパソコン通信による利益を取得できないような出力結果は、そのパソコン通信会員に不利益をもたらすための出力結果としたことを特徴とする請求項1、請求項2または請求項3の個人認証システム。

【請求項5】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザに関する会員データを読み込む会員データ読込工程、会員ユーザに関する会員データを記憶する会員データ記憶工程、会員ユーザが所有するPHS端末装置の存在地域データをPHS事業者から取得する存在地域データ取得工程、会員データと存在地域データとの一致判断を行う演算工程、および演算手段の判断の結果、一致している場合にはサービス提供者からの利益享受を継続できるとともに、不一致の場合にはサービス提供者からの利益を取得できないような出力結果を出力する出力工程を含むことを特徴とする個人認証方法。

【請求項6】クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データを読み込む接続地域データ読込手段、予め接続地域データを記憶している接続地域データ記憶手段、クレジットカード会員が所有するPHS端末装置の存在地域データをPHS事業者から取得する存在地域データ取得手段、存在

地域データに対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータの内容を出力する地域サービスデータ出力手段を備えたことを特徴とする個人認証システム。

【請求項7】地域サービスデータの出力があった場合にはクレジット会員が取引契約を締結できると判断するとともに、地域サービスデータの出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断手段を備えたことを特徴とする請求項6記載の個人認証システム。

【請求項8】クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データおよびカード契約データを読み込むカード契約データ読込工程、クレジットカード会員が所有するPHS端末装置の存在地域データをPHS事業者から取得する存在地域データ読込工程、存在地域データに対応する地域サービスデータの内容を出力する地域サービスデータ出力工程、および地域サービスデータの出力があった場合にはクレジット会員がカード契約を締結できると判断するとともに、地域サービスデータの出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断工程を含むことを特徴とする個人認証方法。

【請求項9】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザの接続地域データを取得する接続地域データ取得手段、会員ユーザが所有する通信端末装置、その通信端末装置の電話番号を予め記憶している電話番号記憶手段、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール手段を備えたことを特徴とする個人認証システム。

【請求項10】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザが所有する通信端末装置の電話番号を予め記憶している電話番号記憶工程、会員ユーザの接続地域データを取得する接続地域データ取得工程、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール工程を備えたことを特徴とする個人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、個人認証システムおよび個人認証方法、更に詳しくは、パソコン通信やクレジットカード等の電子的手段を用いて行う物品購入等の契約において、本人認証をより確実にするためのシステムおよびその方法に関する。

【0002】

【先行技術】従来より、電子的手段を用いての契約、取引などが行われるに際し、その電子的手段を用いている者が正規の契約者であるか否かの認証は、暗証番号、パスワードなどによって行われてきた。例えば、パソコン通信（いわゆるインターネット通信でも同じ）であれば、パソコンおよび電話回線を用いてパソコン通信の会員が申込情報を送信し、事業者側に設置されたコンピュータシステムではこれを受信することで、その両者間の契約を行ってきた。この際、そのパソコン通信会員が正規の契約手順を踏んでいるか否かを認証するため、従来から行われてきている基本的手段は次のようなものである。

【0003】まず、予めパソコンユーザとパソコン通信事業者との間で利用契約を締結する。その際、事業者が正規会員ユーザへ会員ID番号、パスワードを決定して知らせる。事業者は、パソコン通信を介してユーザからアクセス要求があったときには、アクセス者に対して予め登録させた会員IDおよびパスワードを要求し、アクセス者がこれを入力したときに事業者側に記録されている正規会員情報と照合して、これに適合したときには、アクセス者を正規の会員ユーザと認定する。そして、その通信接続中に送信されてくる注文情報等は、その正規の会員ユーザが送信したものと擬制してこれを受け付けるといふものである。

【0004】更に、この正規契約者による正規契約手順が踏まれているか否かの確認をより厳格にするために、事業者側から会員ID番号とパスワードが要求されたときにユーザが入力できる時間を制限したり、誤った入力を一定回数以上行った場合にはこれを不正なアクセス者であると判断して回線を切断する、などの手段によって不正なアクセス者を排除しようとしている。

【0005】

【発明が解決しようとする課題】しかしながら、不正なアクセス者を排除せんとする上記のような方法は、例えばハッカー（不正侵入者）が正規会員ユーザのパソコンの送信ゲートなりモデムなりに侵入し、ここで正規会員ユーザが送信する会員ID番号やパスワードを取得してしまえば、無力化する。予め設定された会員ID番号およびパスワードも何らかの手段で他者が知った場合は、本人認証としてはその役目を果たさなくなる。

【0006】一方、ハッカーによる会員ID番号およびパスワードの不正取得を防止することを目的に、正規会員ユーザと事業者間では情報の伝達を暗号処理し、通信セキュリティを確保して行われることがある。しかし、パスワード等の不正取得を防止する手段を如何に高度化、複雑化させたところで、より高度な不正取得手段を開発するハッカーとの間では何ら本質的な解決策とはならない。

【0007】この類の事件は、従来から銀行カードやク

レジットカードにおいても発生している。特に正規会員ユーザが設定するパスワードは、その忘失を恐れて自己ないしは近親者の誕生日や電話番号の下四桁を活用することも少なくないため、これを悪用しようとする者からすれば比較的容易にパスワードを察知することができ、結果として不正に財貨を取得することができる。

【0008】本発明が解決すべき課題は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない認証技術を提供することにある。ここで、請求項1ないし請求項3および請求項9記載の発明の目的は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証システムを提供することである。

【0009】請求項4記載の発明の目的は、更に、不正なアクセス者に不利益を被らせるようなシステムとすることによって、結果的に不正なアクセス者を未然防止できる個人認証システムを提供することである。請求項5および請求項10記載の発明は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証方法を提供することである。

【0010】請求項6および請求項7記載の発明の目的は、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証システムを提供することである。請求項8記載の発明の目的は、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証方法を提供することである。

【0011】

【課題を解決するための手段】上記した課題を解決するため、本出願人は、前記した請求項1ないし請求項10に記載した発明を提供する。本願に係る発明は、昨今急速に普及しているPHS端末装置、ポケットベル、携帯電話をシステムの正規の会員ユーザが所有していること、且つそのPHS端末装置が常にその正規の会員ユーザの手元に存在していることを前提としている。請求項1ないし請求項8では、PHS端末装置の位置情報入手しているPHS通信事業者からその位置情報を取得し、電子的手段を用いての契約、取引など行おうとしている者がどこにいるかを確認し、通信接続地とPHS端末装置の位置情報とが異なる場合には、これを不正と判断するのである。

【0012】請求項9および請求項10では、PHS端末装置に限られず、ポケットベル、通常の携帯電話の場合も含め、取引直後のコールの有無で不正を判断するのである。

（請求項1）請求項1記載の発明は、情報通信を用いてサービスを提供するサービス提供者（例えば、パソコン

通信事業者AA)が保有するコンピュータに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザに関する会員データを記憶する会員データ記憶手段、会員ユーザに関する会員データ(例えば、会員の住所または居所)を読み込む会員データ読込手段、会員ユーザが所有するPHS端末装置(20)の存在地域データ(D2)をPHS事業者(PP)から取得する存在地域データ取得手段、会員データと存在地域データ(D2)との一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力手段を備えたことを特徴とする。

(用語定義)「会員ユーザ」とは、本発明に係る個人認証システムを利用できる正規の会員であり、本システムを運用するサービス提供者(例えば、パソコン通信事業者(AA)、キャッシュカードを発行する銀行(BB)、クレジットカード会社(CC)など)への登録を済ませた者をいう。クレジットカードが買い物をする際に使用できるようにクレジットカード会社(CC)との契約を済ませた商店(C1)は、ここにいう「会員ユーザ」には含まない。

【0013】会員ユーザがサービス提供者のサービスを受けるには、通信接続手段(10)が必要である。通信接続手段(10)とは、例えばサービス提供者との通信の接続に必要な不可欠な「通信接続信号」を発信する手段のことをいう。本システムがパソコン通信において採用されている場合には、パソコン(12)およびモデム(13)というハードウェアと通信ソフトウェアやパスワードなどのソフトウェアなどをいう。また、本システムがキャッシュカード(15)やクレジットカード(17)による取引において採用されている場合には、カード本体(15,17)とそのカード本体(15,17)に記録されたデータや暗証番号などのソフトウェアなどをいう。銀行のキャッシュカード(15)が使用できるキャッシュディスペンサー(16)やクレジット会社(CC)との契約を済ませた商店(C1)に設置されたカードリーダー(18)は、ここにいう「通信接続手段(10)」の一部を構成する。

【0014】「会員データ」とは、例えば会員ユーザの住所または居所、電話番号など、予めサービス提供者がそのデータベースに蓄えているデータである。「会員データ記憶手段」とは、予めデータを記憶している記憶装置の他、通信接続時に読み込んだデータを記憶する装置も含む場合もある。本発明の個人認証システムがパソコン通信において採用されている場合には、会員ユーザに属する通信接続手段(10)(例えば、パソコン12、モデム13などのパソコン通信機器)を用いてサービス提供者への通信を開始したときの接続地域データ(D1)を「会員データ」とすることができる。更に、その「接続地域データ

(D1)」は、通常はパソコン通信会員の住所または居所であるので、パソコン通信事業者(AA)に登録されており、その会員データのデータベースに蓄積されている。また、この接続地域データ(D1)を、その接続地域のデータとして接続時に読み込むものとすれば、パソコン通信機器を会員ユーザの住所または居所以外の場所に持ち出して接続しても、本発明の個人認証システムは機能することとなる。

【0015】なお、本システムがキャッシュカード(15)やクレジットカード(17)による取引において採用されている場合には、会員データは「接続地域データ(D1)」となり、キャッシュカード(15)やクレジットカード(17)によって取引契約を使用とする支店や店の所在地などとなる。その場合、会員データたる「接続地域データ(D1)」は銀行が管理するコンピュータセンター(BB)やカード会社(CC)に登録されてデータベースに蓄積されているとともに、銀行支店や商店(C2)に設置されたキャッシュディスペンサー(16)やカードリーダー(18)からコンピュータセンター(BB)やカード会社(CC)へ発信される。

【0016】「存在地域データ(D2)」とは、通信時にPHS端末装置(20)が使用することができるPHS基地局(例えばP1)の所在地のことであり、PHS基地局(例えばP1)が受信したものを使用する。通常は、PHS端末装置(20)とPHS基地局(P1)とは、絶えず定期的に基地局IDを電波にて送受信している。本システムを運用するサービス提供者(AA)は、この基地局IDにて認識できる存在地域データ(D2)を、PHS基地局(P1)を介してPHS事業者(PP)から取得する。

【0017】本システムがパソコン通信において採用されている場合であって、図3に示すように会員ユーザが当該PHS端末装置(20)をパソコン(12)のモデム(13)に接続してパソコン通信を行った場合、「存在地域データ」は、その通信を接続したPHS基地局(P3)の所在地とすることができる。「演算手段」とは、例えば「会員データ」と「存在地域データ」が単純なデータである場合には、両データの解釈とテーブルによる対応とを行う装置をも含む趣旨である。例えば、図1に示すように複数のPHS基地局(P1,P2)による存在地域データ(D2)が読み込まれる可能性がある場合には、「会員データと存在地域データとの一致判断」は、補正手段などによって一致していると判断する。

【0018】「不一致の場合の出力結果」とは、通常は、通信または取引を継続することができないように回線を接続することであるが、通信を継続することによって不利益をもたらされるような出力であってもよい。例えば、クレジットカードを無効とするためにカードの記録データを書き換えるためのデータ出力などが該当する。なおこれに付随して、正規の会員に対して、不正に使用されているおそれがある旨を、信用機関等を通じて連絡することとしてもよい。

【0019】請求項1記載の発明に係る個人認証システムによれば、以下のような作用をなす。まず、会員ユーザがサービス提供者(AA)への通信を開始し、本発明に係る個人認証システムは会員データ読込手段にて会員データを読み込む。また、サービス提供者(AA)は、会員ユーザが所有するPHS端末装置(20)の存在地域データ(D2)を、存在地域データ取得手段にてPHS事業者(PP)から出力によって読み込む。そして、記憶手段によって予め記憶している会員データと存在地域データ(D2)との一致判断を、演算手段によって行う。

【0020】このとき、会員ユーザは自分が所有するPHS端末装置(20)を手元に置いてあるとすると、演算手段は会員データと存在地域データ(D2)とが一致していると判断する。その場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザであると判断し、出力手段によって会員ユーザはサービス提供者(AA)からの利益享受を継続できる。

【0021】一方、その演算手段が会員データと存在地域データ(D2)とが一致していないと判断した場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザでないと判断する。すると、出力手段によってその通信を開始した者は、サービス提供者(AA)からの利益を取得できない。サービス提供者(AA)への通信を開始した者の手元に、正規の会員ユーザが所有するPHS端末装置(20)が存在しないこととなっており、不正なアクセスである可能性が極めて高いからである。

【0022】以上のように、会員ユーザに対して本発明に係る個人認証システムが新たに強いる負担は、自分が所有するPHS端末装置(20)を手元に置いておくことのみである。これは、会員ユーザに対しての負担にはならない。携帯用通信端末機の性格上、自分が所有するPHS端末装置(20)を手元に置いておくことはあたりまえだからである。

(請求項2) 請求項2記載の発明は請求項1記載の発明をパソコン通信の場合に限定したものであり、サービス提供者をパソコン通信事業者とし、会員データは、パソコン通信の接続電話番号によって認識することとしたことを特徴とする。

【0023】会員データを、会員登録時のパソコン通信会員の住所または居所とすると、携帯用パソコンを用いて自宅以外の場所から通信すると正規の会員でないと判断されてしまう。また、転居をした場合には、その度に届け出をしなければならない。そこで、通信のアクセスポイントの接続電話番号を会員データ(接続地域データD1)として認識することとしたものである。パソコン通信会員は、パソコン通信に要する電話料金が最も安いアクセスポイントへ接続するのが一般的だからである。

(請求項3) 請求項3記載の発明は、請求項2記載の発明を技術的に限定したものであり、接続地域データ(D1)

は、パソコン通信会員がパソコン通信の接続時に入力することとしたことを特徴とする。

【0024】携帯用パソコンによって通信する場合、接続地域データがパソコン通信会員の住所または居所ではないことがありえる。その場合、請求項2のように接続地域データを定めることもできるが、会員に直接入力してもらうのが本請求項記載の発明である。通信速度の関係で、アクセスポイントを電話料金が最も安いものとしがない場合があるからである。

10 (請求項4) 請求項4記載の発明は、請求項1、請求項2または請求項3の発明を技術的に限定したものであり、演算の結果が不一致の場合にパソコン通信による利益を取得できないような出力結果は、そのパソコン通信会員に不利益をもたらすための出力結果としたことを特徴とする。

(用語定義) 「不利益をもたらすため出力結果」とは、通信を継続できなかったり終了させてしまうという消極的な出力結果のほか、当該パソコンの使用者の利益を積極的に害するような出力のことである。例えば、通信に用いているパソコンをフリーズさせたり、当該パソコンに警告表示画面を表示させるためのソフトウェアなどである。

【0025】請求項4記載の発明によれば、前記請求項記載の発明と異なり、以下のような作用をなす。すなわち、演算手段が接続地域データ(D1)と存在地域データ(D2)とが一致していないと判断した場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザでないと判断する。そして、その通信を開始した者は、出力手段によって不利益を被る。この不利益を被るおそれの告知により、結果として不正なアクセス者を未然防止することができる。

(請求項5) 請求項5記載の発明は、情報通信を用いてサービスを提供するサービス提供者(AA)が保有するコンピュータに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザに関する会員データを読み込む会員データ読込工程、会員ユーザに関する会員データを記憶する会員データ記憶工程、会員ユーザが所有するPHS端末装置(20)の存在地域データ(D2)をPHS事業者(PP)から取得する存在地域データ取得工程、会員データと存在地域データ(D2)との一致判断を行う演算工程、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力工程を含むことを特徴とする。

(請求項6) 請求項6記載の発明は、クレジットカード会員のカード(17)を用いてカード会社(CC)への通信することによって接続地域データ(D1)を読み込む接続地域デ

ータ読込手段、予め接続地域データ(D1)およびカード契約データを記憶している契約データ記憶手段、クレジットカード会員が所有するPHS端末装置(20)が使用可能な最寄りのPHS基地局からの出力によって存在地域データ(D2)を読み込む存在地域データ取得手段、存在地域データ(D2)に対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータ(D3)の内容を出力する地域サービスデータ出力手段を備えたことを特徴とする個人認証システムである。

(用語定義)「クレジットカード会員のカード(17)を用いてカード会社(CC)への通信する」とは、カードリーダー(18)および電話(14)または専用回線などの通信回線を用いて、かかるカード(17)の有効期限等のチェックを行うなどのための通信を行うことをいう。

【0026】「地域サービスデータ(D3)」とは、PHSアンテナ基地局(P1)が位置する地域に関し、PHS端末装置(20)のカード会員にとって有益な情報のことである。具体的には、最寄り駅名、最寄りのパソコン通信アクセスポイントの電話番号などPHS端末装置(20)の表示画面やスピーカーによって出力可能な簡単且つ短いデータや、携帯用パソコンなどに接続して取り出すような大きなデータ、例えば近傍の地図、地域ショッピングガイドなどである。ただし、クレジットカードを使用しようとした者が正規のクレジットカード会員か否かを確かめるための出力であるので、短い出力であることが多い。特に、買い物済ませた会員に対しての情報であるので、最寄り駅名、その最寄り駅の終電車時刻、当該クレジットカードが使用できる最寄りの商店のイベント情報などが有益である。

【0027】地域サービスデータ(D3)は、図6に示すように、カード会員の所有するPHS端末装置(20)をその出力装置としてもよいし、図8に示すように、クレジットカード会社(CC)との契約を済ませた商店(C1)が所有する機器に出力することとしてもよい。PHS端末装置(20)の電話番号は、「クレジットカード会員のカード(17)を用いてカード会社(CC)への通信する」際に、カードリーダー(18)、電話(14)など機器を用いて送信することとしてもよい。その場合、カード使用者が正規のカード会員でない場合にはPHS端末装置(20)の電話番号を商店の店員に告げる際に躊躇することとなる。

【0028】次に、請求項6記載の発明の作用を説明する。まず、クレジットカード会員のカード(17)を用いてカード会社(CC)への通信を開始し、本発明に係る個人認証システムは接続地域データ読込手段にて接続地域データ(D1)を読み込む。また、カード会社(CC)は、クレジットカード会員が所有するPHS端末装置(20)の存在地域データ(D2)を、存在地域データ取得手段にて最寄りの基地局(例えばP1)から出力によって読み込む。そして、存在地域データ(D2)に対応する地域サービスデータ(D3)を地域サービスデータ記憶手段から出力する。

【0029】このとき、カード使用者が正規のクレジットカード会員であるとする、地域サービスデータ(D3)を受け取ることとなり、商店側はそのカード使用者が正規のクレジットカード会員であると判断できる。その後、取引契約を締結すればよい。一方、カード使用者が正規のクレジットカード会員でないとする、地域サービスデータ(D3)を受け取れないことを理由として、商店側はそのカード使用者が正規のクレジットカード会員でないとして判断できる。クレジットカード(17)のみを不正に取得した者がそのカード(17)を使用している可能性が極めて高いからである。

【0030】請求項1記載の発明と同じように、会員ユーザに対して本発明に係る個人認証システムが新たに強い負担は、自分が所有するPHS端末装置(20)を手元に置いておくことのみである。これは、会員ユーザに対しての負担にはならない。携帯用通信端末機の性格上、自分が所有するPHS端末装置(20)は手元にあるのが普通だからである。

(請求項7) 請求項7記載の発明は、請求項6記載の発明を技術的に限定したものであり、地域サービスデータ(D3)の出力があった場合にはクレジット会員が取引契約を締結できると判断するとともに、地域サービスデータ(D3)の出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断手段を備えたことを特徴とする。

【0031】すなわち、請求項6の構成要件に「判断手段」を加えたものである。換言すると、請求項6記載の発明において「判断手段」を必須構成要件としていないのは、かかる判断を人為手段、すなわち商店の店員が行うこととする場合があるからである。

(請求項8) 請求項8記載の発明は、クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データ(D1)およびカード契約データを読み込むカード契約データ読込工程、クレジットカード会員が所有するPHS端末装置(20)が使用可能な最寄りのPHS基地局からの出力によって存在地域データ(D2)を読み込む存在地域データ読込工程、存在地域データ(D2)に対応する地域サービスデータ(D3)の内容を出力する地域サービスデータ出力工程、および地域サービスデータ(D3)の出力があった場合にはクレジット会員がカード契約を締結できると判断するとともに、地域サービスデータ(D3)の出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断工程を含むことを特徴とする個人認証方法である。

(請求項9) 請求項9記載の発明は、情報通信を用いてサービスを提供するサービス提供者が保有するコンピュータに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザの接続地域データを取得する接続地域データ

取得手段、会員ユーザが所有する通信端末装置、その通信端末装置の電話番号を予め記憶している電話番号記憶手段、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール手段を備えたことを特徴とする。

【0032】ここで、「通信端末装置」とは、PHS、いわゆるポケットベルの他、通常の携帯電話をも含む趣旨である。

〈請求項10〉情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザが所有する通信端末装置の電話番号を予め記憶している電話番号記憶工程、会員ユーザの接続地域データを取得する接続地域データ取得工程、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール工程を備えたことを特徴とする。

【0033】

【発明の実施の形態】以下、本発明を実施の形態および図面に基づいて更に詳しく説明する。ここで使用する図面は図1ないし図10である。図1は、本発明の第一の実施の形態を示す概念図である。図2は、本発明の第一の実施の形態を示すフローチャートである。図3は、本発明の第二の実施の形態を示す概念図である。図4は、本発明の第三の実施の形態を示す概念図である。図5は、本発明の第四の実施の形態を示す概念図である。図6は、本発明の第五の実施の形態を示す概念図である。図7は、本発明の第五の実施の形態を示すフローチャートである。図8は、本発明の第六の実施の形態を示す概念図である。図9は、本発明の第七の実施の形態を示す概念図である。図10は、本発明の第七の実施の形態を示すフローチャートである。

（第一の実施の形態）まず、図1および図2に基づいて、本発明の第一の実施の形態を説明する。この第一の実施の形態は、情報通信を用いてサービスを提供するパソコン通信事業者Aが保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合に採用されるシステムであって、接続者が正規の会員ユーザであるか否かを認証する個人認証システムおよび個人認証方法である。

【0034】パソコン通信事業者Aの提供するサービスを受けるためには、氏名、住所または居所、電話番号などをパソコン通信事業者Aに登録し、この登録を済ませた者が会員ユーザとなる。パソコン通信事業者Aは、そのデータベース(DB)に会員ユーザに関する会員データ（例えば、会員の住所または居所）を記録しておく。会員ユーザは、パソコン通信事業者Aの提供するサービスを受けるため、パソコン12、モデム13および電話14というハードウェアと通信ソフトウェア

や、パソコン通信事業者Aとの間で決められたパスワード等を用いて、通信を接続する。接続は、パソコン通信事業者Aが提供するアクセスポイントA1、A2、A3、・・・の中から、距離や通信速度などを勘案して適当なものを選んで行う。

【0035】一方、本システムにおいては、会員ユーザがPHS端末装置20を所有していることを前提としている。したがって通常、パソコン通信事業者Aは、そのPHSの電話番号や識別番号をも会員データとして登録、記憶している。PHS事業者（PP）は、エリア内に多数の基地局P1、P2、P3、・・・を設置しており、それぞれの基地局P1、P2、P3からはPHS端末装置20に対して、現在のPHS端末装置20の位置によればどの基地局を使用するか、という情報を電波により発信している。したがって、どのPHS端末装置20が、どの基地局の近傍に存在するかという存在地域の情報を取得できる。

【0036】パソコン通信事業者Aは、あるユーザがパソコン通信に接続を開始した場合、そのユーザに対応する会員データを会員データ読込手段によって読み込む。この実施の形態にあつては、接続があつたユーザのパスワード等から、データベース(DB)に記憶された会員データにアクセスしてその住所または居所を読み込む。

【0037】一方、その会員ユーザが所有するPHS端末装置20の存在地域の情報たる存在地域データD2を、PHS事業者（PP）から取得する。なお、最寄りの基地局としてP1、P2の二つがある場合、電波Q1、Q2のいずれを存在地域データD2とするかは、PHS事業者（PP）またはパソコン通信事業者Aに設けられた補正手段によって定められるものとする。

【0038】パソコン通信事業者Aは、会員データと存在地域データD2との一致判断を行う演算手段を備えており、その演算手段によって両データの一致を判断する。判断の結果、一致している場合にはパソコン通信事業者Aからの利益享受を継続できるとともに、不一致の場合にはパソコン通信事業者Aからの利益を取得できないような出力結果を出力する。この実施の形態にあつては、パソコン通信をパソコン通信事業者A側から一方的に終了させるという出力をする。

【0039】会員ユーザは自分が所有するPHS端末装置20を手元に置いてあるとすると、演算手段は会員データと存在地域データD2とが一致していると判断する。その場合、本実施の形態に係る個人認証システムは、通信を開始した者が正規の会員ユーザであると判断し、出力手段によって会員ユーザはパソコン通信による利益享受を継続できる。

【0040】一方、その演算手段が会員データと存在地域データ(D2)とが一致していないと判断した場合とは、通信を開始した者の手元に正規の会員ユーザが所有する



PHS端末装置20が存在しないということである。自分が所有するPHS端末装置20が手元にないという事態は通常はあり得ないことであり、不正なアクセスである可能性が極めて高いからである。

(第二の実施の形態) 続いて、図3に基づいて第二の実施の形態について説明する。

【0041】第一の実施の形態にあっては、接続があったユーザのパスワード等から会員データにアクセスしてその住所または居所を読み込むこととしているので、PHS端末装置20を持って外出し、携帯用のパソコンによって住所または居所以外のところで通信を開始すると、会員データと存在地域データD2とが一致しないと判断されてしまう。そこで、第二の実施の形態にあっては、予めデータベースに記憶されている会員の住所または居所を会員データとしては用いず、アクセスポイントA1から接続したことを、その電話番号などと置き換え、その接続地域データD1を会員データとして読み込むこととする。この接続地域データD1を、その接続地域のデータとして接続時に読み込むものとするれば、パソコン通信機器を会員ユーザの住所または居所以外の場所に持ち出して接続しても、この個人認証システムは機能することとなる。

【0042】なお、接続地域データD1を上記のようにして決めることもできるが、会員に直接入力してもらうこともできる。通信速度の関係で、アクセスポイントを電話料金が最も安いものとししない場合があるからである。

(第三の実施の形態) 続いて、図4に基づいて第三の実施の形態について説明する。

【0043】この第三の実施の形態は、個人認証システムが銀行のキャッシュカード15による取引において採用される場合である。「会員データ」は接続地域データD1、すなわちキャッシュカード15によって取引契約を行う銀行支店B1の所在地である。図4は、キャッシュカード15によってキャッシュディスペンサー16から現金を引き出す場合を説明している。

【0044】キャッシュカード15をキャッシュディスペンサー16へ挿入し、暗証番号を入れたとすると、そのキャッシュディスペンサー16は接続地域データD1をコンピュータセンターBBへ送る。一方、コンピュータセンターBBは、キャッシュカード15の正規の持ち主のPHS端末装置20の存在地域データD2をPHS事業者(PP)から取得し、接続地域データD1と存在地域データD2との一致を判断する。そして、一致していると判断すれば現金を引き出せ、一致していないと判断すれば引き出せないような出力結果を、キャッシュディスペンサー16へ出力する。

(第四の実施の形態) 続いて、図5に基づいて第四の実施の形態について説明する。

【0045】この第四の実施の形態は、個人認証システ

ムがクレジット会社CCのクレジットカード17による取引において採用される場合である。「会員データ」は接続地域データD1、すなわちクレジットカード17が使用できるカード利用契約を結んだ商店C1の所在地である。図5は、クレジットカード17によって商品を購入する際に、クレジットカード17の有効期限などを照会するカードリーダー18による読み込みの場合を説明している。

【0046】カードリーダー18によってクレジットカード17の磁気情報が読み込まれたとすると、その情報は電話4(または専用回線)を介してクレジット会社CCへ送る。一方、クレジット会社CCは、カード契約データを読み込むとともに、クレジットカード17の正規の持ち主のPHS端末装置20の存在地域データD2をPHS事業者(PP)から取得し、接続地域データD1と存在地域データD2との一致を判断する。そして、一致していると判断すればそのクレジットカード17が使用でき、一致していないと判断すればそのクレジットカード17が使用できないとする出力結果を、カードリーダー18へ出力する。

(第五の実施の形態) 続いて、図6および図7に基づいて第五の実施の形態について説明する。この第五の実施の形態は、個人認証システムがクレジット会社CCのクレジットカード17による取引において採用される場合であって、第四の実施の形態の変形例である。

【0047】第五の実施の形態が第四の実施の形態と異なるのは、クレジットカード17の使用が所有するはずのPHS端末装置20へサービスデータを出力するというシステムを有する点である。更に詳しく説明する。

第五の実施の形態は、存在地域データD2に対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータの内容をクレジットカード会員のPHS端末装置20へ地域サービスデータD3を出力する地域サービスデータ出力手段を備えている。

【0048】更に、カードリーダー18には、PHS端末装置20と接続して地域サービスデータD3の出力があったかどうかの判断をする判断手段19が備えられている。ここで「地域サービスデータD3」とは、PHSアンテナ基地局P1が位置する地域に関し、PHS端末装置20のユーザにとって有益な情報のことである。具体的には、買い物を済ませたユーザに対しての情報であるので、最寄り駅名、その最寄り駅の終電車時刻、当該クレジットカードが使用できる最寄りの商店のイベント情報などである。

【0049】このような実施の形態にあっては、カード使用者が正規のクレジットカード会員であるとする、手元のPHS端末装置20から地域サービスデータD3を受け取り、そのことを判断手段19が判断することによって、商店側はそのカード使用者が正規のクレジットカード会員であると判断できる。その後、取引契約を締

結すればよい。一方、カード使用者が正規のクレジットカード会員でないとすると、判断手段19が手元のPHS端末装置20から地域サービスデータD3を受け取れないと判断するはずであり、商店側はそのカード使用者が正規のクレジットカード会員でないと判断できる。クレジットカード17のみを不正に取得した者がそのカード17を使用している可能性が極めて高いからである。

(第六の実施の形態) 続いて、図8に基づいて第六の実施の形態について説明する。

【0050】この第六の実施の形態は、個人認証システムがクレジット会社CCのクレジットカード17による取引において採用される場合であって、第五の実施の形態の変形例である。第五の実施の形態と異なる点は、地域サービスデータD3を、商店C1が所有する機器、例えばカードリーダー18に接続して設けたスピーカ19Aへ出力することとした点である。その出力が行われない、または商店C1の存在する地域にそぐわないものであれば、そのクレジットカード17による取引を中止する。

【0051】上記してきた第一ないし第六の実施の形態において個人認証のために会員ユーザに要求されることは、PHS端末装置20を手元に置いておくことのみであり、新たに暗証番号を覚えたり、新しい鍵を持ち歩いたりすることを強いるものではない。

(第七の実施の形態) 続いて、図9および図10に基づいて第七の実施の形態について説明する。

【0052】この第七の実施の形態は、個人認証システムがクレジット会社CCのクレジットカード17による取引において採用される場合であって、構成をシンプル化し、更にPHS端末装置だけではなく、ポケットベルや通常の携帯電話も使用できるようにした個人認証のためのシステムである。この第七の実施の形態は、会員ユーザのPHS端末装置20の電話番号を予めデータベースに記憶している。そして、取引をしようとする会員ユーザのクレジットカード17をカードリーダー18で読み、会員ユーザの接続地域データD1を商店C1の電話14など通信回線から取得する。接続地域データD1を取得したクレジットカード会社CCは、データベースに記憶された会員ユーザの電話番号を読み込み、PHS端末装置20へ認証のための電話をかける。

【0053】会員ユーザのPHS端末装置20に認証のための電話がクレジット会社CCからかかってくれば、店員はその電話がかかってきたことで、目の前の会員ユーザが正規の会員であると推定して取引を成立させればよい。認証コールがなければ、目の前の会員ユーザが正規の会員でないかもしれないと推定し、カードでの取引ができない旨を伝えればよい。

【0054】なお、この実施の形態では携帯通信端末としてPHS端末装置20を採用したが、ポケットベルや通常の携帯電話でもよい。第七の実施の形態において個

人認証のために会員ユーザに要求されることは、クレジットカード会社CCにデータ登録した携帯通信端末装置(この例においてはPHS端末装置20)を手元に置いておくことのみであり、新たに暗証番号を覚えたり、新しい鍵を持ち歩いたりすることを強いるものではない。

【0055】

【発明の効果】請求項1ないし請求項3および請求項9記載の発明によれば、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証システムを提供することができた。請求項4記載の発明によれば、更に、不正なアクセス者に不利益を被らせるようなシステムとすることによって、結果的に不正なアクセス者を未然防止できる個人認証システムを提供することができた。

【0056】請求項5記載および請求項10によれば、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証方法を提供することができた。請求項6および請求項7記載の発明によれば、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証システムを提供することができた。

【0057】請求項8記載の発明によれば、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証方法を提供することができた。

【図面の簡単な説明】

【図1】本発明の第一の実施の形態を示す概念図である。

【図2】本発明の第一の実施の形態を示すフローチャートである。

【図3】本発明の第二の実施の形態を示す概念図である。

【図4】本発明の第三の実施の形態を示す概念図である。

【図5】本発明の第四の実施の形態を示す概念図である。

【図6】本発明の第五の実施の形態を示す概念図である。

【図7】本発明の第五の実施の形態を示すフローチャートである。

【図8】本発明の第六の実施の形態を示す概念図である。

【図9】本発明の第七の実施の形態を示す概念図である。

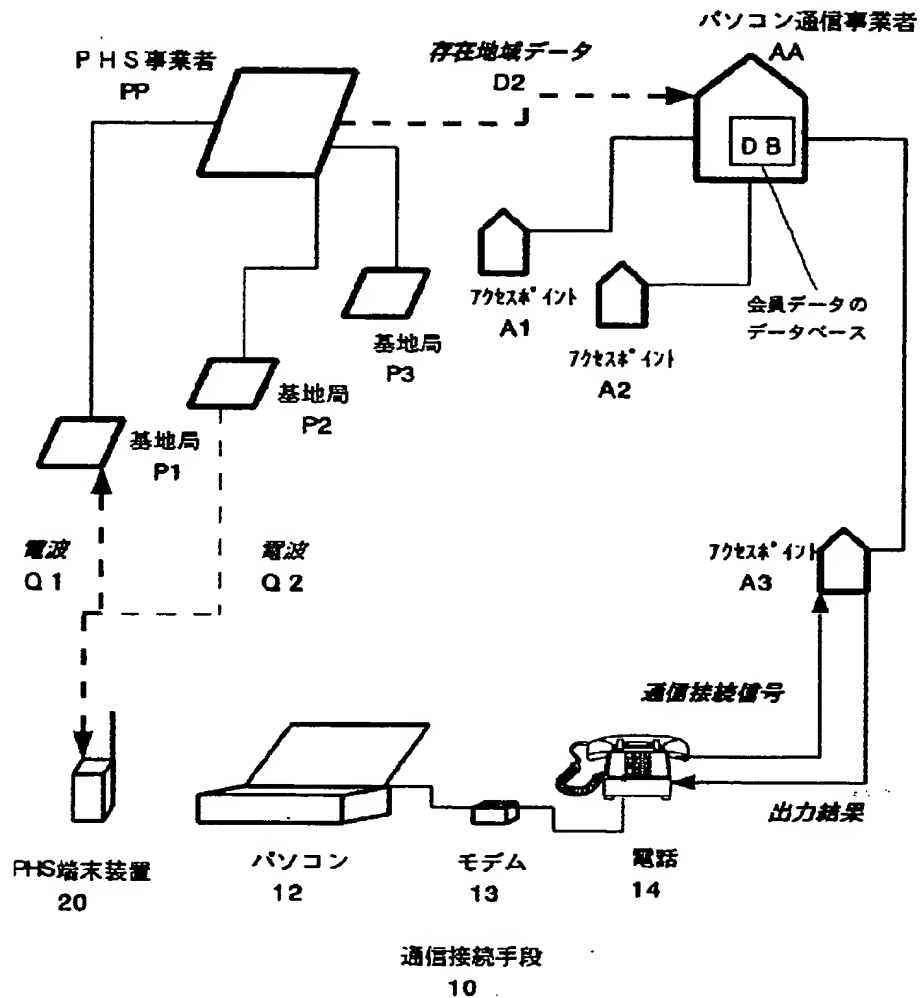
【図10】本発明の第七の実施の形態を示すフローチャートである。

【符号の説明】

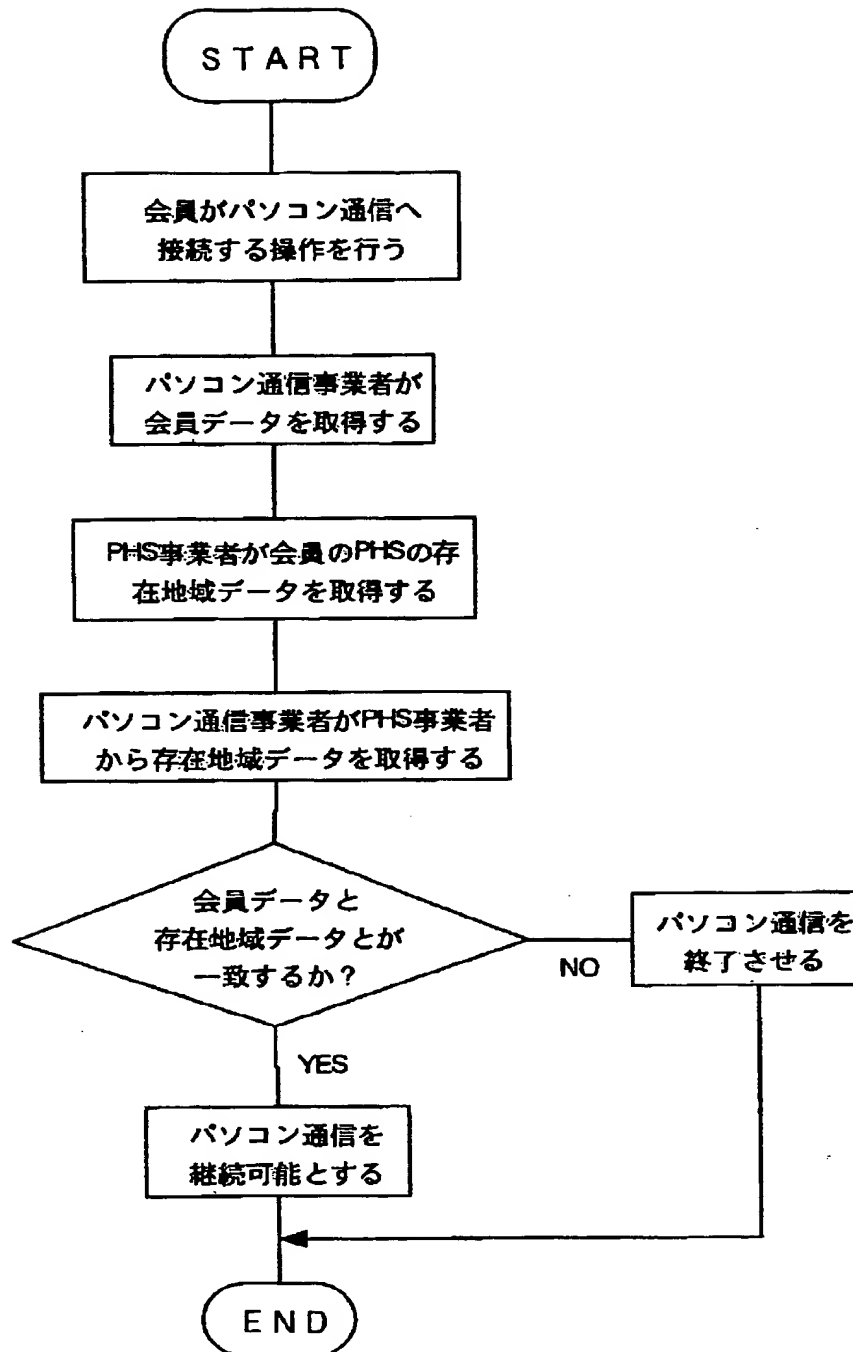
10 通信接続手段

17		18	
12	パソコン	13	モデム * A1, A2, A3
14	電話		BB 銀行が管理するコンピュータセンター
16	キャッシュカード	15	キャッシュ B1 銀行支店
16	キャッシュディスペンサー		CC クレジット会社
18	カードリーダー	17	クレ C1 商店
19	判断手段		D1 接続地域データ
20	PHS端末装置		地域データ D2 存在
AA	パソコン通信事業者	19A	スビ D3 地域サービスデータ
			PP PHS事業者
		10	P1, P2, P3 基地局
		*	Q1, Q2 電波

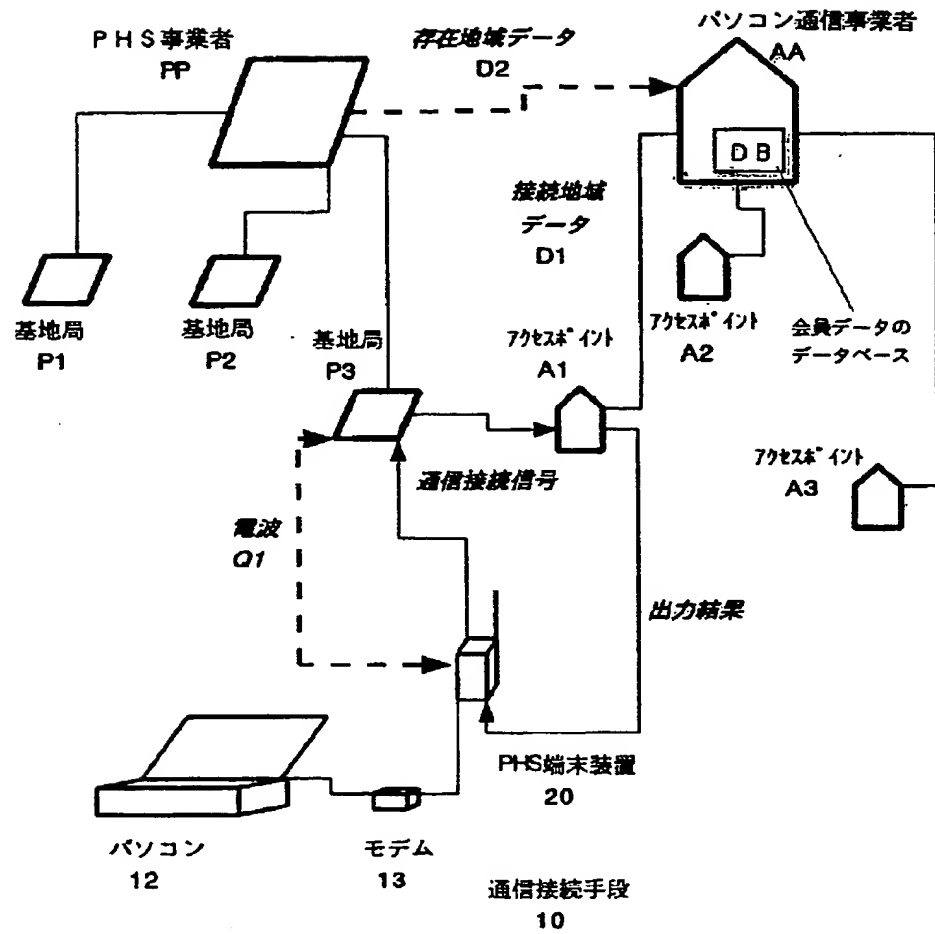
【図1】



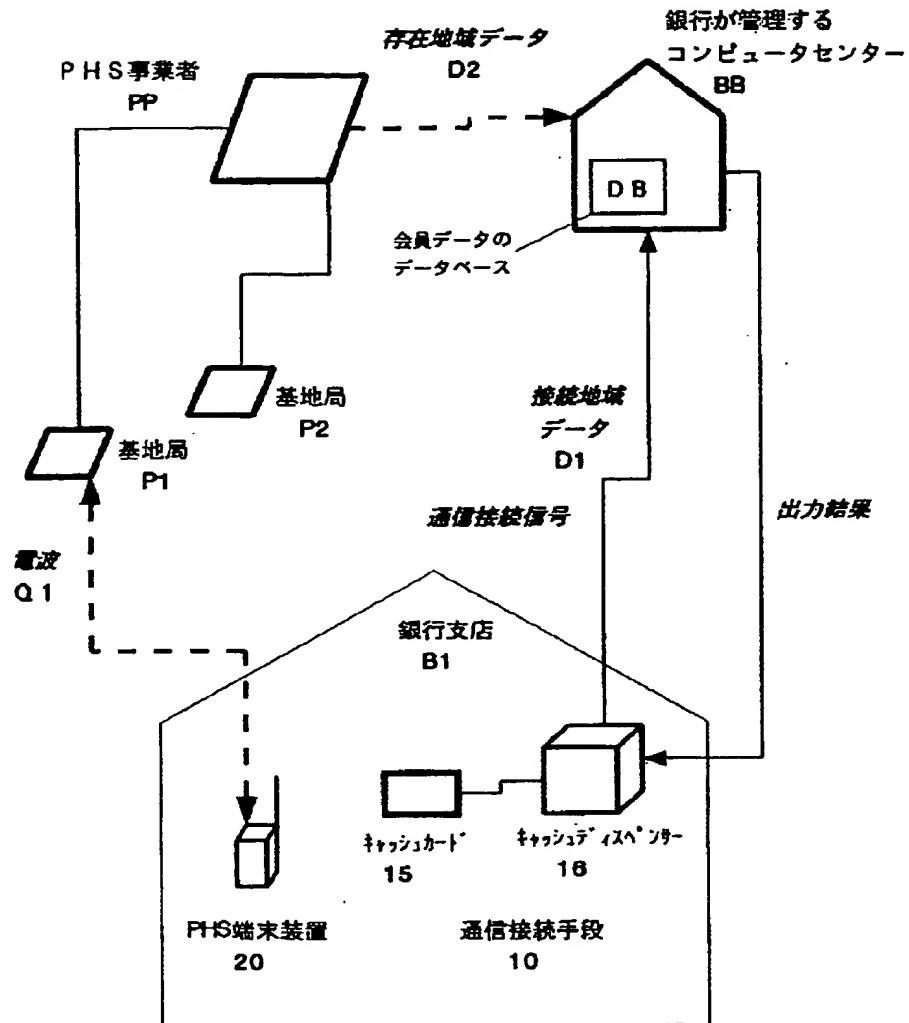
【図2】



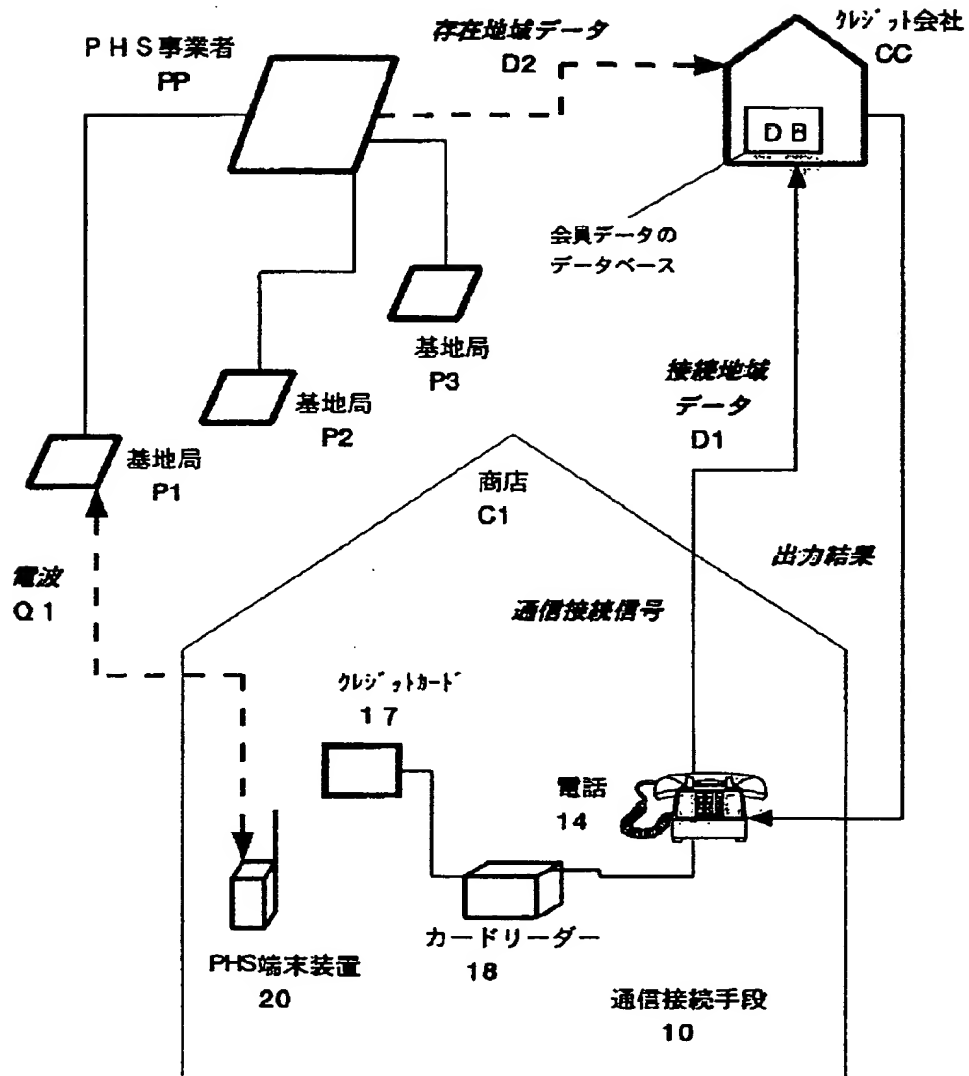
【図3】



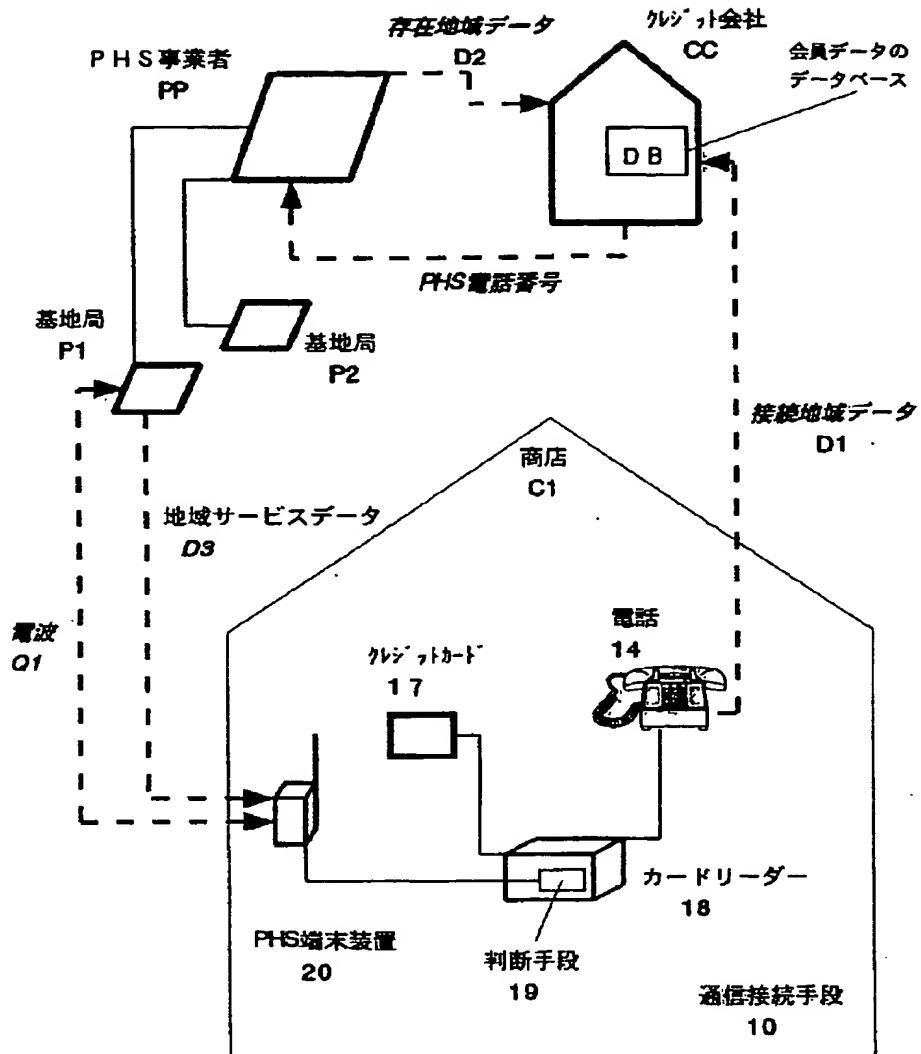
【図4】



【図5】

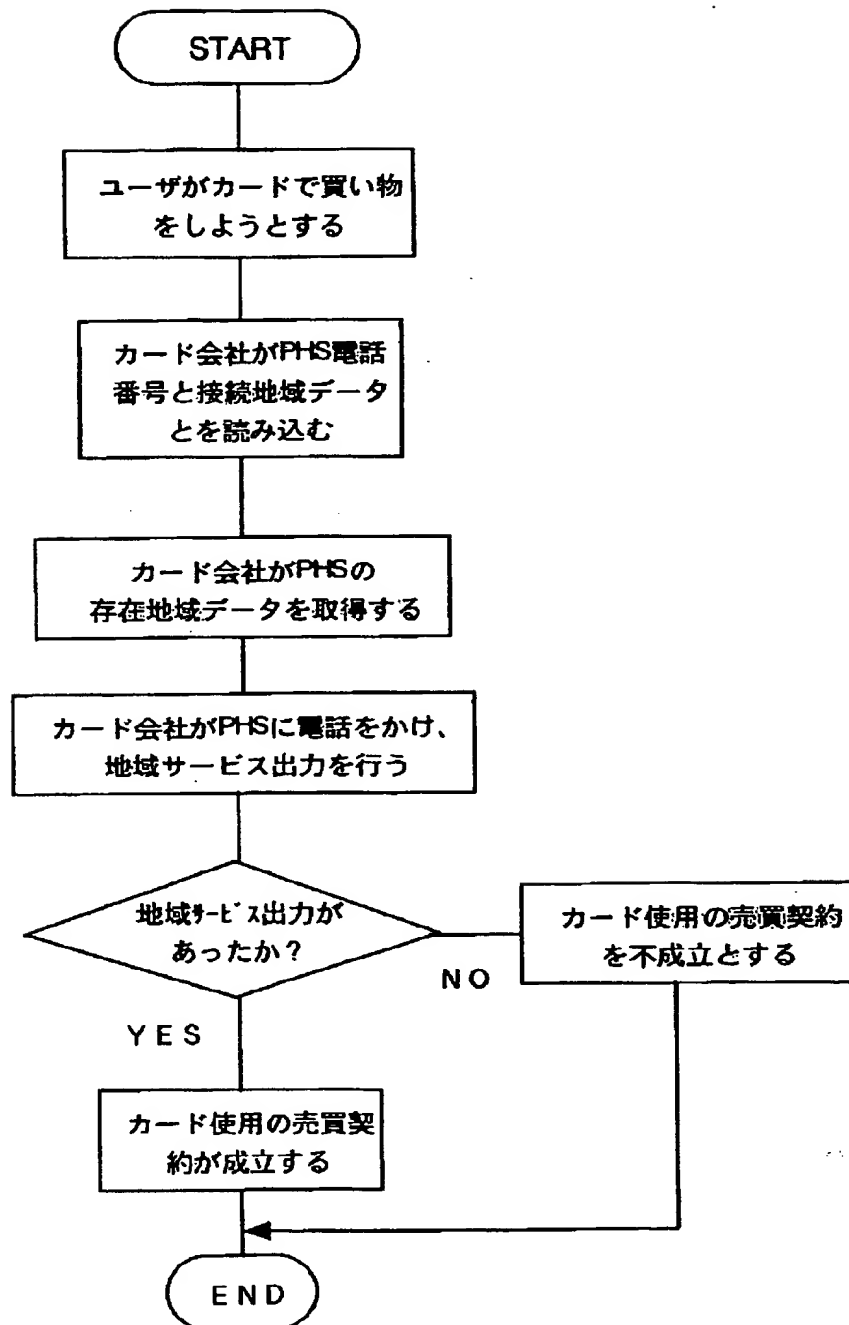


【図6】

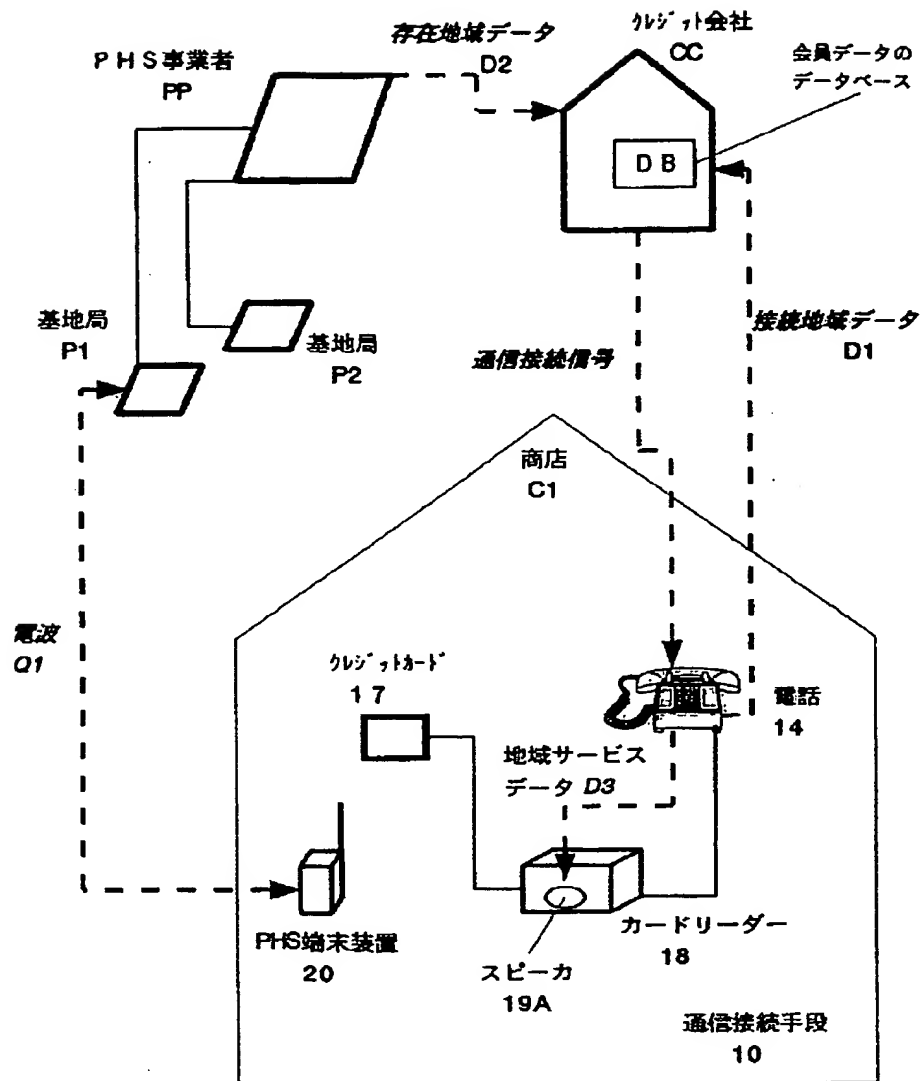




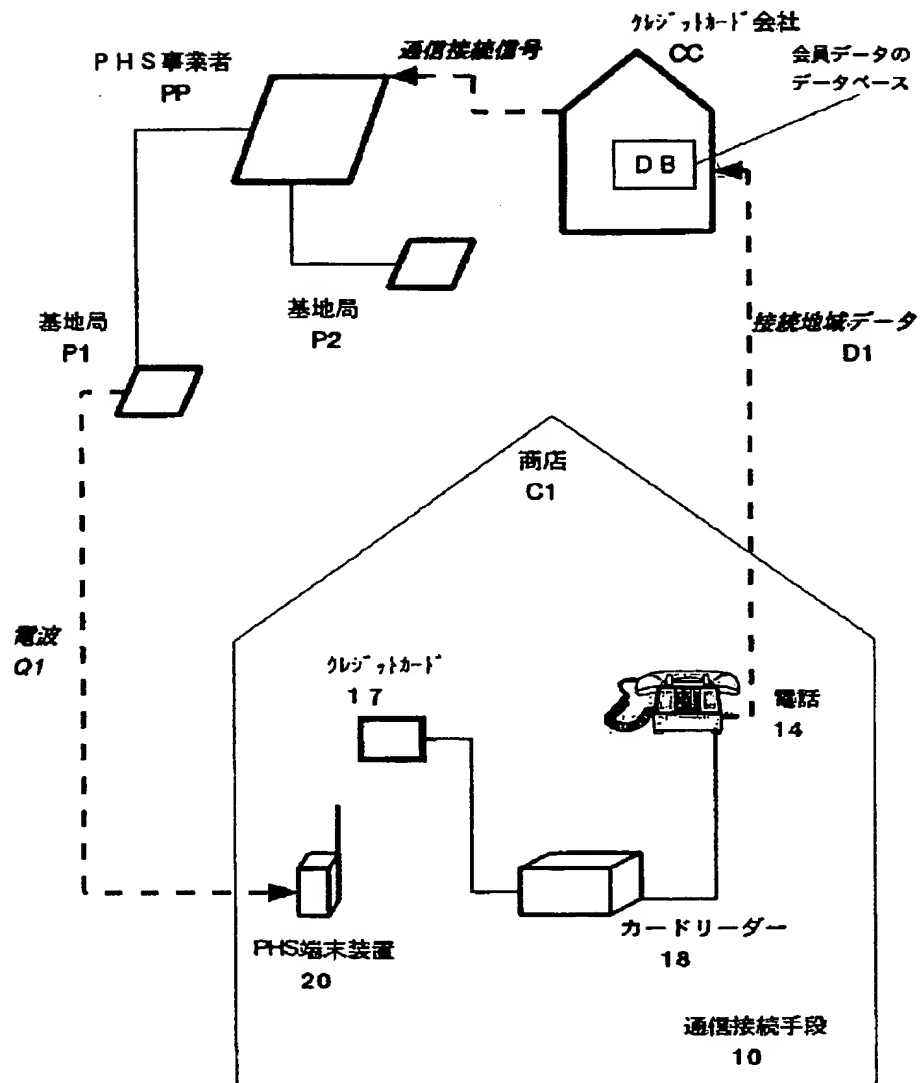
【図7】



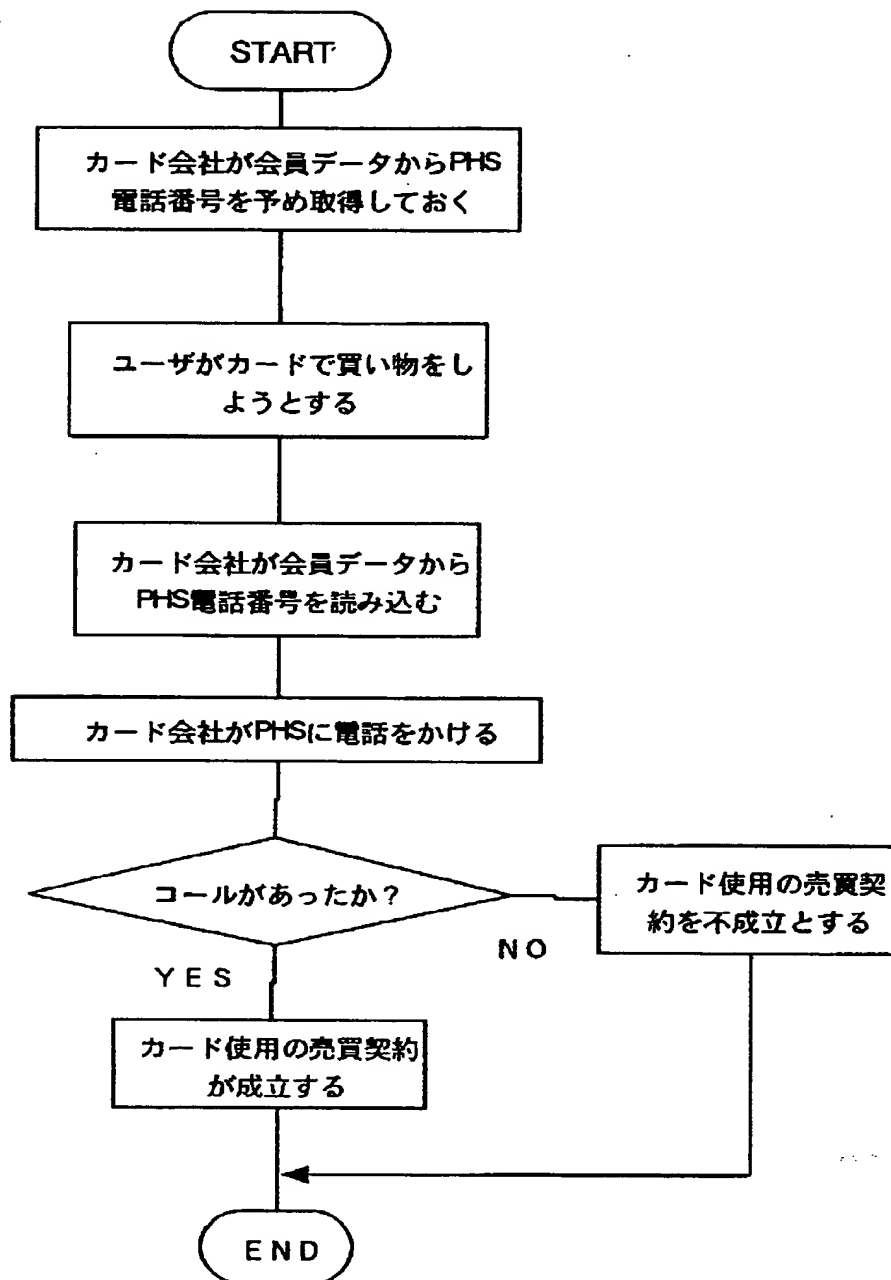
【図8】



【図9】



【図10】



フロントページの続き